: **Michigan Department of Labor and Economic Growth**

Agency Report to the

JOINT COMMITTEE ON ADMINISTRATIVE RULES

Rev. 2002

Rule: R 500.551 – R 500.560 (proposed)
Agency: DLEG – Office of Financial & Insurance Services

1. Name, address, FAX and phone numbers of agency contact person:

Dorothy Cherry, 611 W. Ottawa, 3rd Floor, Lansing, MI 48933 (517) 241-2073, Fax (517) 335-1727, dcherr@Michigan.gov

2. Purpose for the proposed rules and background:

The proposed rules will bring Michigan into full compliance with the privacy and safeguarding provisions of Title V of the Gramm-Leach-Bliley Act (GLBA), 15 USC 6801 et. seq., enacted November 12, 1999, with most substantive privacy provisions taking effect July 1, 2001. Section 505(b) of the GLB Act, 15 USC 6805, requires state insurance authorities to implement **by rule** the appropriate administrative, physical, and technical safeguards to protect the security and confidentiality of customers' nonpublic personal information as required by Section 501(b), 15 USC 6801. Both cited sections are part of Title V of the GLB Act and apply to all financial service providers, whether regulated by federal or state authorities. The federal agencies – OCC, OTS, FDIC, Federal Reserve, FTC, NCUA, and SEC – all adopted privacy regulations in 2000 and all adopted safeguarding guidelines or rules in 2001 and 2002.

Michigan enacted Chapter 5 of Insurance Code in 2001 PA 24, MCL 500.501 to 500.547, effective July 1, 2001, to implement the privacy requirements of Title V, and the purpose of the proposed rules is to implement the safeguarding requirements, as directed in MCL 500.547: "The Commissioner shall adopt guidelines for administrative, technical, and physical safeguards that protect the security, confidentiality, and integrity of customer information, **pursuant to** sections 501, 505(b), and 507 of the Gramm-Leach-Bliley act, Public Law 106-102, 113 Stat. 1338, 15 U.S.C. 6801. 6805, and 6807." As noted above, a " Guideline . . . pursuant to" GLBA is, by definition in 15 USC 6805(b), a "rule" and not a Michigan Administrative Procedures Act guideline. MCL 24.203(6) defines "guideline" as "an agency statement or declaration of policy which the agency intends to follow, which does not have the force or effect of law, and which binds the agency but does not bind any other person." Obviously, a Michigan APA guideline would make no sense in terms of a federal requirement that Michigan implement and enforce safeguarding standards on regulated insurance entities.

It is true that the federal banking agencies (OCC, OTS, Federal Reserve, and FDIC) did adopt Interagency Guidelines to implement the safeguarding standards as part of safety and soundness standards, but GLBA specifically authorized such action by the federal banking agencies, and those agencies enforce as law their safety and soundness standards. GLBA Section 505(b), 15 USC 6805(b) directs the SEC, the FTC, and state insurance authorities (i.e. all non-banking agencies) to implement the safeguarding standards "by rule." The SEC final safeguarding rule, Regulation S-P, 17 CFR 248.30, became effective July 1, 2001, and the

FTC final safeguarding rule (adopted in 2002) became effective May 23, 2003. As of January 2004, 23 states (AL, AR, CA, CO, CT, DE, FL, IL, IA, ME, MO, NE, NH, NY, NC, OR, PA, SD, UT, VT, VA, WV, WY) and the District of Columbia have adopted similar safeguarding administrative rules, all based on the National Association of Insurance Commissioners (NAIC) model safeguarding rule as are Michigan's proposed rules. Similar rules are pending adoption in Arkansas and New Jersey.

GLBA Section 505(c), 15 USC 6805(c), states that if Michigan fails to adopt a safeguarding rule as required, Michigan shall not be eligible to override the federal insurance customer protection regulations under Section 45(a) of the Federal Deposit Insurance Act.

In short, the purpose of the proposed safeguarding rules is to comply with federal law and to prevent the invalidation of other Michigan insurance consumer protection laws for failure to comply.

3. Summary of proposed rules:

The proposed rules establish appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer nonpublic personal financial information under 15 USC 6801 et. seq. and Chapter 5 of the Insurance Code, MCL 500.501 et. seq.

4. Name and date of publication in newspapers (minimum 3):

Lansing State Journal, February 11, 2004; Traverse City Record-Eagle, February 11, 2004; The Houghton Daily Mining Gazette, February 11, 2004

5. Time, date, location and duration of public hearing:

10:00 a.m., March 2, 2004, Lake Superior Room – Ground Floor, Michigan Library and Historical Center, 702 West Kalamazoo, Lansing, Michigan. Duration: 1 hour, until 11 a.m.

6. Date of publication of rules and public hearing notice in *Michigan Register:*

Issue #2, February 15, 2004

7. Agency persons attending hearing (include agency name and title of position):

Christine Nettleton - Departmental Specialist. Dorothy Cherry – Administrative Law Specialist

8. Names, organizations and (complete) addresses of persons attending the hearing:

Lawrence J. Kish, Esq.
Life Ins. Assn. of Michigan
230 N. Washington #306
Lansing, MI 48933
(517-482-7058)

Christine Shearer
MI Assn of Health Plans
327 Seymour Ave.
Lansing, MI 48933
(517-371-3181)

Kurt Gallinger, Esq.
American Insurance Assn.
124 W. Allegan, Suite 800
Lansing, MI 48933
(517-374-9171)

Eric Henning, Esq.
MI Insurance Coalition
124 W. Allegan, Suite 800
Lansing, MI 48933
(517-374-9185)

Teri Morante
Citizens Ins. Co.
645 W. Grand River
Howell, MI
(517-540-2288)

Dyck VanKoevering, Esq.
Insurance Institute of MI
112 East Allegan
Lansing, MI
(517-371-2880)

Jim Miller
Farm Bureau Ins.
7373 W. Saginaw
Lansing, MI
(517-323-7000 – 2044)

Colleen Curtis
JCAR
P.O. Box 30036
Lansing, MI 48909
(517-373-9327)

9. Persons submitting letters, comments and testimony of support:

All speakers at the public hearing expressed general support for the idea safeguarding customer information, but no one expressed support for the entire rule set as proposed.

10. Persons submitting letters, comments and testimony of opposition:

Jennifer Kildea Dewane, Esq. (letter)
For Jackson National Life Insurance Co.
Foster, Swift, Collins & Smith, P.C.
313 S. Washington Square
Lansing, MI 48933-2193
(517-371-8211)

Lawrence J. Kish (testimony & letter)

Kurt Gallinger, Esq. (testimony)

Christine Shearer (letter)

J. Stephen Zielezienski (letter)

Rick Lantz (letter)

American Insurance Association
1130 Connecticut Ave. NW, Suite 1000
Washington, DC 20036

Delta Dental
P.O. Box 30416
Lansing, MI 48909-7916

John P. Gerni (letter)
American Council of Life Insurers
1708 Thicket Court
Fort Wayne, IN 46814
(260-625-5386)

11. Summary on suggestions to modify proposed rules:

Suggestion to modify:

a) Mr. Gallinger, Mr. Zielezienski, (both for American Insurance Association), Ms. Dewane (for Jackson National), Mr. Kish (for the Life Insurance Assn. of Michigan), Mr. Gerni (for American Council of Life Insurers), Mr. Henning (for Michigan Insurance Coalition) and Ms. Shearer (for Michigan Association of Health Plans) all assert that OFIS should not be promulgating rules under the Michigan Administrative Procedures Act (APA), MCL 24.201 et. seq., to implement Gramm-Leach-Biley safeguarding standards when MCL 500.547 begins, "The Commissioner shall adopt guidelines. . . " The argument is that guidelines are a specific agency action, defined in the Michigan APA, subject to different sections, different notice requirements, and resulting in legal effects different from rules. Guidelines do not have the force and effect of law and bind only on the Commissioner and the agency. Thus, the objection is that OFIS essentially has no authority to promulgate a rule when the Legislature has clearly directed "guidelines" as the administrative action the Commissioner must take.

Agency response:

a) The agency does not agree and thinks substantial confusion has arisen from the difference between a guideline under the Michigan Administrative Procedures Act, without the force and effect of law, and a guideline issued by a federal banking agency, which does have the force and effect of law. MCL 500.547 must be read in its entirety. MCL 500.547 directs the Commissioner to adopt guidelines, ". . . pursuant to sections 501, 505(b), and 507 of the Gramm-Leach-Bliley act, . . . 15 U.S.C. 6801, 6805, and 6807." Thus, the statutory reference on "guidelines" is not to Michigan's Administrative Procedures Act at all, but to the federal law cited; and 15 U.S.C. 505(b) specifically requires "the applicable state insurance authority" to "implement the standards prescribed under section 501(b) **by rule** with respect to the financial institutions and other persons subject to their respective jurisdictions under subsection (a)." Section 505, 15 U.S.C. 6805, is the Enforcement section of Title V on privacy; and the state insurance authority must enforce both the privacy and the safeguarding provisions of Title V. It is true that the federal banking agencies adopted Interagency

Guidelines to safeguard customer information under GLBA, Federal Register, Vol. 66. No 22, February 1, 2001; but those federal banking guidelines are part of federal banking safety and soundness standards that the OCC, OTS, Federal Reserve, and FDIC have full power to enforce as law. 15 U.S.C. 505 specifically requires the non-banking federal agencies (SEC, NCUA, FTC), like state insurance authorities, to implement the safeguarding standards **by rule.** Since a Michigan APA "guideline" binds only the Commissioner and agency, a guideline on safeguarding standards would not be enforceable against the financial institutions subject to the Commissioner's jurisdiction and would not fulfill the US congressional mandate of Title V of the GLB Act. The Commissioner thinks a properly promulgated APA rule is the only way to follow the legislative direction of MCL 500.547 to implement the administrative, physical, and technical safeguards "**pursuant to**" the Gramm-Leach-Bliley act. The absence of GLBA required state action has significant consequences. Under 15 U.S.C. 6805(c), failure to follow the GLBA mandate would make Michigan ineligible to preserve its own state law insurance customer protections.

To clarify this issue, the agency recommends changing the authority recital in parentheses at the top of the first page of the proposed rules to delete "in accordance with," and include "pursuant to," i.e. the federal language. The agency also recommends for clarity changing R 500.551(c) to add the words "by rule" after the word "implement."

Suggestion to modify:

b) Mr. Zielezienski (both for American Insurance Association) and Ms. Dewane (for Jackson National) argue that MCL 500.2047 requires the Commissioner to hold a "trade practice conference" before promulgating a rule creating an unfair trade practice.

Agency response:

b) The agency recommends deleting the reference to MCL 500.2047 in the authority recital on page 1 of the proposed rules and substituting MCL 500.210, the section granting the commissioner general rule making authority.

Suggestion to modify:

c) Mr. Zielezienski (for American Insurance Association) requests deletion from Rule 2, R 500.552, the mistaken reference to MCL 500.503(o) as bearing no relation to the defined term.

Agency response:

c) Thank you, Mr. Zielezienski! The correct reference is to MCL 500.503(p) and the definition there of "personally identifiable financial information." The Agency recommends correcting this citation in the proposed rules.

Suggestion to modify:

d) Mr. Gallinger and Mr. Zielezienski (for American Insurance Association), Mr. Kish (for the Life Insurance Association of Michigan, and Mr. Gerni (for the American Council of Life Insurers) request deletion of Rules 5through 9, R 500.555 through 500.559, the examples portion of the safeguarding standards, on grounds that the use of any examples "creates the appearance of a standard to follow" and/or that R 500.555(2) diminishes the statement in R 500.555(1) that the examples provided are non-exclusive.

Agency response:

d) The agency does not recommend revision of these sections. The proposed rules follow the NAIC model regulation, both in providing examples and in the examples given, thus providing a Michigan rule consistent with that applied to insurers and licensees in other states. Other financial service providers, subject to the federal guidelines of the banking agencies (OCC, OTS, Federal Reserve, FDIC) or subject to the rules promulgated by the non-banking agencies (SEC, NCUA, FTC) are required to have written information security programs containing all the elements provided as examples in R 500.555 through 500.559. The purpose of the examples is, in fact, to create a standard to follow, as required by Section 505(b)(2) of the Gramm Leach Bliley Act. The agency added R 500.555(2) at the suggestion of the Legislative Service Bureau to give both direction and assurance to licensees that the agency shall consider the implementation actions specified in the examples compliance. Thus, a licensee may develop a written information security program as specified in R 500.553 and R 500.554 either by following the example implementation actions specified in R 500.555 through R 500.559 or by alternative actions or means. R 500.555(2) simply notifies licensees of implementation actions the agency approves as establishing compliance. A licensee who develops and selects alternative implementation actions or means is likewise notified that the agency has made no determination as whether or not such alternatives establish compliance.

Suggestion to modify:

e) Mr. Gallinger and Mr. Zielezienski (for American Insurance Association), Mr. Kish (for Life Insurance Assn. of Michigan), and Mr. Henning (for Michigan Insurance Coalition) request deletion separately of R. 500.558, on grounds that the Commissioner has no authority to adopt rules requiring licensees to police the activities of their service providers. In the alternative, Mr. Zielezienski requests deletion of R 500.558(b) even if R 500.558(a) is retained, on grounds that due diligence in selection of a service provider, as required by subsection (a), will likewise permit a licensee to determine if a service provider should be retained, as required by subsection (b.)

Agency response:

e) The agency does not recommend revision of this portion of the rule. Both subsections are included in the NAIC model and should be retained for uniformity. The NAIC rejected the same objections raised here. Essentially this section recites, by way of example, that any licensee should consider data security capabilities in selecting, contracting with, and retaining service providers. Six of the seven federal agencies

implementing safeguarding standards also included provisions involving overseeing service provider arrangements. The agency does not believe it unreasonable to expect a business with a statutory duty to maintain the privacy and security of certain customer financial information to include provisions regarding data security in its contracts with service providers and to monitor those contracts. Moreover, MCL 500.533 specifically limits the scope of disclosures to service providers, and these rules require no more "policing" than required by the statutes they implement - GLBA and Chapter 5 of the Insurance Code.

Suggestion to modify:

f) Mr. Gallinger, Mr. Zielezienski, Mr. Kish, Mr. Henning, Ms. Dewane, and Ms. Shearer (for Michigan Association of Health Plans) all object to the portion of R 500.560 that states that a violation of the safeguarding standards shall constitute a knowing violation as defined in MCL 500.2038(1)(a).

Agency response:

f) The agency recommends revision of Rule 10, R 500.560, to create a subparagraph (a) for that section to read as follows:

AS PROVIDED IN MCL 500.2013, a violation of any requirement of these rules is an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this state.

Suggestion to modify

g) Mr. Kish (for the Life Insurance Association of Michigan) and Mr. Gerni (for the American Council of Life Insurer) both object to the R 500.551(d) requirement that entities possessing both nonpublic personal financial information and health and medical information must either segregate the information subject to different security standards or apply the more stringent administrative, technical, and physical safeguards to all types of sensitive customer information: financial, health and medical. Mr. Gerni asserts that the compliance obligations of life insurers (not HIPAA "covered entities") are unclear from the language of R 500.551(d). Ms. Shearer (for the Michigan Association of Health Plans) and Mr. Lantz (for Dental Dental) suggest the addition of Section 20 of the NAIC privacy model, providing that compliance with the federal Heath Insurance Portability and Accountability Act (HIPAA) privacy standards (45 CFR Parts 160 & 164) excludes a licensee from being subject to Chapter 5 of the Insurance Code and the proposed safeguarding rules.

Agency response:

g) While not agreeing entirely with all comments made on this section, the agency does agree that compliance with HIPAA security standards, including any more stringent provisions of Michigan law specifically preserved by HIPAA, for all customer information - financial, health, and medical - should constitute compliance for a licensee with Chapter 5 of the Insurance Code on nonpublic personal financial information only and these proposed rules. The HIPAA security standards, found at 45 CFR 164.302 through 164.318, are included within the privacy rule promulgated by

the U.S. Department of Health and Human Services, effective April 14, 2003 for all but small health plans, and effective April 14, 2004 for small health plans. Also, recent amendments to the federal Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 et seq., include enhanced protection for medical information included in consumer credit reports. Licensees that are not HIPAA-covered entities such as life insurers may well have security duties under other federal and state laws apart from or in addition to HIPAA and FCRA; and all licensee duties to comply with such other laws are specifically preserved by MCL 500.501 and R 500.551(d).

The agency recommends amending R 500.551(d) to eliminate the segregation requirement and to reference other laws potentially applicable to customer information in each licensee's possession. The agency has elected to retain the final sentence of R 500.501(d) as notice of one Michigan law more stringent that HIPAA, FCRA, and Chapter 5 of the Insurance Code.

The agency also recommends adding R 500.560(b) to state specifically that a licensee's compliance with HIPAA privacy and security standards, including any more stringent provisions of Michigan law, for all customer information in a licensee's possession, shall constitute compliance with the provisions of Chapter 5 of the Insurance Code, MCL 500.501-500.547 and these safeguarding rules. Addition of this section should eliminate any concern over duplicate standards.

The revisions of R 500.551(d) read as follows:

(d) Section 507 provides, among other things, that a state may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. MCL 500.501(3) provides that Chapter 5 of the Insurance Code - applicable to financial information - does not modify, limit, or supersede statute or rules governing the confidentiality or privacy of individually identifiable health or medical information under state law. To release such PRIVATE OR PRIVILEGED health or medical information IN MICHIGAN generally requires the informed, written consent of the patient or his OR HER authorized representative. ~~and n~~ Nothing in these rules shall be construed to diminish state law, ~~or~~ recent federal HIPAA standards (45 CFR Parts 160 and 164) that govern the ~~confidentiality and~~ privacy AND SECURITY of ~~individually identifiable~~ PROTECTED health and medical information, OR FAIR CREDIT REPORTING ACT PROTECTIONS FOR MEDICAL INFORMATION (15 U.S.C. 1681 et seq.) The safeguards established pursuant to these rules ~~shall~~ apply ONLY to nonpublic personal financial information AND DO NOT DIMINISH THE DUTY OF ANY LICENSEE TO COMPLY WITH OTHER MORE STRINGENT STATE OR FEDERAL LAWS AFFECTING OTHER TYPES OF CUSTOMER INFORMATION IN LICENSEE'S POSSESSION. ~~All licensees gathering or in possession of both nonpublic personal financial information and nonpublic personal health and medical information shall either segregate the different types of information subject to different security standards or shall apply the more stringent administrative, technical, and physical safeguards, otherwise applicable to individually identifiable health and medical information under state or federal law, to all types of customer nonpublic personal information and records - financial, health and medical to ensure the~~

~~security and confidentiality of all sensitive information. In addition to the civil penalties the Commissioner may impose for violation of these rules under Chapter 20 of the Insurance Code, MCL 500.2001 to 500.2050,~~ FOR EXAMPLE, licensees are notified that MCL 750.410 (2) establishes criminal penalties for any person, firm, or corporation that buys, sells, furnishes, or receives "for any consideration" the identity of a patient or any information concerning treatment unless otherwise authorized by law, administrative rule, or valid legal process.

The agency further recommends adding R 500.560(b) to read as follows:

(b) IF A LICENSEE COMPLIES WITH ALL REQUIREMENTS OF THE FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY (HIPAA) PRIVACY RULE, INCLUDING SECURITY STANDARDS AND ANY MORE STRINGENT STATE LAWS, 45 CFR PARTS 160 AND 164, FOR ALL CUSTOMER INFORMATION IN LICENSEE'S POSSESSION - FINANCIAL, HEALTH, AND MEDICAL - SUCH COMPLIANCE SHALL ALSO CONSTITUTE COMPLIANCE WITH CHAPTER 5 OF THE INSURANCE CODE, MCL 500.501 TO 500.547, AND THESE SAFEGUARDING RULES.

`

Name of person completing this report: **Dorothy Cherry** (Print)

_____ (Signature)

Date of report: June 24, 2004